DOCKET NO: 241199US6

IN THE UNITED STATES PATENT & TRADEMARK OFFICE

IN RE APPLICATION OF	:
HIDEO SATO	: EXAMINER: TOLENTINO, R.
SERIAL NO: 10/633,658	:
FILED: AUGUST 5, 2003	: GROUP ART UNIT: 2134
FOR: ENCRYPTION APPARATUS	:

APPEAL BRIEF

COMMISSIONER FOR PATENTS
ALEXANDRIA, VIRGINIA 22313

SIR:

This is an appeal from the decision of the Examiner dated July 30, 2007 which finally rejected Claims 1-20 in the above-identified patent application. A Notice of Appeal was timely filed on October 30, 2007.

I. REAL PARTY-IN-INTEREST

The real party-in-interest is Sony Corporation.

II. RELATED APPEALS AND INTERFERENCES

Appellants, Appellants' legal representative, and the assignees are aware of no prior or pending appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

Claims 1-20 have been finally rejected and form the basis for this appeal. Appendix VIII includes a clean copy of Claims 1-20.

IV. STATUS OF AMENDMENTS

No amendments after final rejection were filed.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent Claim 1 is directed to an encryption apparatus for performing an encryption operation using a public key encryption technique. The encryption apparatus includes public key encryption processing means for performing an encryption operation on data using a public key encryption technique to generate encrypted data (Figure 6 and page 26, line 22 to page 27, line 24, and ECC Block 360_1, Figures 12A-12D), hash value generation means for generating a hash value which is used by the public key encryption processing means (SHA-1 Block 360_1, Figures 12A-12D and page 39, lines 17-21), storage means for storing the hash value (ALU RAM 370, Figures 12A-12D and page 40, lines 11-12), and control means for controlling the hash value generation means and the public key encryption processing means (ECC/SHA-1 Block 360_1, Figures 12A-12D and page 40, lines 2-14). The control means suppresses arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means. (Page 40, lines 11-12)

Independent Claim 13 is directed to an encryption apparatus for performing an encryption operation using a public key encryption technique. The encryption apparatus includes a public key encryption processing unit configured to perform an encryption operation on data using a public key encryption technique to generate encrypted data (Figure

6 and page 26, line 22 to page 27, line 24, and ECC Block 360_1, Figures 12A-12D), a hash value generation unit configured to generate a hash value which is used by the public key encryption processing unit (SHA-1 Block 360_1, Figures 12A-12D and page 39, lines 17-21), a storage unit configured to store the hash value (ALU RAM 370, Figures 12A-12D and page 40, lines 11-12), and a control unit configured to control the hash value generation unit and the public key encryption processing unit (ECC/SHA-1 Block 360_1, Figures 12A-12D and page 40, lines 2-14). The control unit is configured to suppress arithmetic operations performed by the public key encryption processing unit when the hash value generation unit accesses the storage unit. (Page 40, lines 11-12)

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The grounds of rejection to be reviewed on appeal are

(a) whether Claims 1, 2, 5, 6, 9, 11, 13, 14, 17, and 18 are unpatentable under 35 U.S.C. §103(a) over Garib (U.S. Patent No. 6,728,378) in view of Dyer et al. (U.S. Patent No. 6,625,592, hereinafter "Dyer");

(b) whether Claims 3, 4, 15, and 16 are unpatentable under 35 U.S.C. §103(a) over Garib in view of Dyer and further in view of Kaufman et al. (U.S. Patent No. 5,764,772, hereinafter "Kaufman");

(c) whether Claims 7 and 19 are unpatentable under 35 U.S.C. §103(a) over Garib in view of Dyer and further in view of Kitamura (U.S. Patent Application Publication No. 20020016917);

(d) whether Claims 8 and 20 are unpatentable under 35 U.S.C. §103(a) over Garib in view of Dyer and Kitamura and further in view of Kaufman;

(e) whether Claim 10 is unpatentable under 35 U.S.C. §103(a) over Garib in view of Dyer and further in view of Schneier (Applied Cryptography, Second Edition); and

(f) whether Claim 12 is unpatentable under 35 U.S.C. §103(a) over Garib in view of Dyer and further in view of Inada (U.S. Patent No. 6,986,044).

VII. ARGUMENTS

A. Claims 1, 2, 5, 6, 9, 11, 13, 14, 17, and 18 are not unpatentable over Garib in view of Dyer

Claim 1 recites in part, "control means for controlling the hash value generation means and the public key encryption processing means, the control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means."

The outstanding Office Action conceded that Garib does not teach or suggest this feature, and cited Dyer as describing this subject matter.[1] Dyer describes a method of searching a memory by storing data entries arranged using hash values. Dyer describes that the hash values for multiple data entries can be computed sequentially or in parallel.[2] However, this description of sequential processing only relates to the ***computation*** of hash values for ***other data entries***. It is respectfully submitted that Dyer does not describe the suppression of any actions while a hash function accesses a storage means, much less suppressing public key encryption processing means when a hash function ***accesses a storage means***. In fact, as Dyer describes searching a memory using hash values, Dyer certainly does not teach or suggest public key encryption processing means.

The Advisory Action of October 16, 2007 reasserted that column 5, lines 14-20 and column 2, lines 7-21 of Dyer describe the above quoted feature, specifically stating "Dyer teaches having information be worked out on in parallel or separate times. By choosing to

[1] See the outstanding Office Action at page 3, lines 5-18.
[2] See Dyer, column 5, lines 14-20.

perform the steps not in parallel, it will suppress the operations being done by any other process including operations performed for the public key."

Initially, it is again noted that Dyer only describes the parallel or serial processing of hash values for entries of a search table. Dyer does not explicitly describe that any operations are suppressed. Accordingly, the Advisory Action is apparently asserting that Dyer inherently describes such a feature. However, the Advisory Action does not meet the requirements to establish inherency. As noted in MPEP §2112, "To establish inherency, ***the extrinsic evidence 'must make clear that the missing descriptive matter is necessarily present in the thing described in the reference, and that it would be so recognized by persons of ordinary skill.*** Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient.'" *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950-51 (Fed. Cir. 1999) (Emphasis added.).

In the present case, ***no evidence of any kind*** has been provided to establish that "control means for controlling the hash value generation means and the public key encryption processing means, the ***control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means***" is inherent in the disclosure of Dyer. Therefore, Dyer does not teach or suggest "control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means ***accesses the storage means***" as defined in Claim 1.

Further, the motivation provided by the outstanding Office Action is irrelevant to the invention recited in Claim 1. The outstanding Office Action states "it would have been obvious to a person of ordinary skill in the art to use Dyer's system for hash scanning of shared memory interfaces with Garib's secret key messaging because it offers the advantage of being faster to traverse the hash memory (Dyer, Col. 2 Lines 7-21)." However, the claimed invention does not traverse multiple entries in a hash memory. The claimed invention uses a hash value for ***encryption*** purposes. Thus, there is no motivation for one of ordinary skill in the art to look at the searching mechanism of Dyer, much less to combine it with Garib's invention.

The Advisory Action of October 16, 2007 again cited column 2, lines 7-21 of Dyer as describing the claimed subject matter. Again, the invention of Dyer, a search engine which searches using hash values for each entry of a linked list, is irrelevant to the claimed invention, and does not include any operations including a public key. Thus, the statement the outstanding Advisory Action that "By choosing to perform the steps not in parallel, it will suppress the operations being done by any other process including operations performed for the public key" is unsupported by the disclosure of Dyer. Therefore, it is again respectfully submitted there is no suggestion or motivation to combine Garib and Dyer.

Consequently, as Garib and Dyer do not teach each and every element of Claim 1, and there is no suggestion or motivation to combine Garib and Dyer, Claim 1 (and Claims 2-12 dependent therefrom) is patentable over Garib and Dyer.

Claim 13 recites in part "a control unit configured to control the hash value generation unit and the public key encryption processing unit, the control unit configured to suppress arithmetic operations performed by the public key encryption processing unit when the hash value generation unit accesses the storage unit."

As noted above, Dyer does not describe, either especially or inherently, that any particular operation is suppressed when a hash function accesses a storage unit, much less suppressing arithmetic operations performed by a public key encryption processing unit when a hash value generation unit accesses a storage unit. As further noted above, there is no suggestion or motivation to combine Garib and Dyer. Consequently, as Garib and Dyer do not teach each and every element of Claim 13, and there is no suggestion or motivation to combine Garib and Dyer, Claim 13 (and Claims 14-20 dependent therefrom) is also patentable over Garib and Dyer.

B. Claims 3, 4, 15, and 16 are not unpatentable over Garib in view of Dyer and further in view of Kaufman

With regard to the rejection of Claims 3, 4, 15, and 16 as unpatentable over Garib in view of Dyer and further in view of Kaufman, it is noted that Claims 3 and 4 are dependent from Claim 1 and Claims 15 and 16 are dependent from Claim 13, and thus are believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kaufman does not cure any of the above-noted deficiencies of Garib and Dyer. Accordingly, it is respectfully submitted that Claims 3, 4, 15, and 16 are patentable over Garib in view of Dyer and further in view of Kaufman.

C. Claims 7 and 19 are not unpatentable over Garib in view of Dyer and further in view of Kitamura

With regard to the rejection of Claims 7 and 19 as unpatentable over Garib in view of Dyer and further in view of Kitamura, it is noted that Claim 7 is dependent from Claim 1 and Claim 19 is dependent from Claim 13, and thus are believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kitamura does not cure any of the above-noted deficiencies of Garib and Dyer. Accordingly, it is respectfully submitted that Claims 7 and 19 are patentable over Garib in view of Dyer and further in view of Kitamura.

D. Claims 8 and 20 are not unpatentable over Garib in view of Dyer and Kitamura and further in view of Kaufman

With regard to the rejection of Claims 8 and 20 as unpatentable over Garib in view of Dyer and Kitamura and further in view of Kaufman, it is noted that Claim 8 is dependent from Claim 1 and Claim 20 is dependent from Claim 13, and thus are believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Kitamura and Kaufman do not cure any of the above-noted deficiencies of Garib and Dyer. Accordingly, it is respectfully submitted that Claims 8 and 20 are patentable over Garib in view of Dyer and Kitamura and further in view of Kaufman.

E. Claim 10 is not unpatentable over Garib in view of Dyer and further in view of Schneier

With regard to the rejection of Claim 10 as unpatentable over Garib in view of Dyer and further in view of Schneier, it is noted that Claim 10 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Schneier does not cure any of the above-noted deficiencies of Garib and Dyer. Accordingly, it is respectfully submitted that Claim 10 is patentable over Garib in view of Dyer and further in view of Schneier.

F. Claim 12 is not unpatentable over Garib in view of Dyer and further in view of Inada

With regard to the rejection of Claim 12 as unpatentable over Garib in view of Dyer and further in view of Inada, it is noted that Claim 12 is dependent from Claim 1, and thus is believed to be patentable for at least the reasons discussed above. Further, it is respectfully submitted that Inada does not cure any of the above-noted deficiencies of Garib and Dyer.

Accordingly, it is respectfully submitted that Claim 12 is patentable over Garib in view of Dyer and further in view of Inada.

Conclusion

It is respectfully requested that the outstanding rejections be REVERSED.

Respectfully submitted,

OBLON, SPIVAK, McCLELLAND,
MAIER & NEUSTADT, P.C.

Edward Tracy

Bradley D. Lytle
Attorney of Record
Registration No. 40,073

Edward W. Tracy, Jr.
Registration No. 47,998

Customer Number
22850

Tel: (703) 413-3000
Fax: (703) 413 -2220
(OSMMN 08/07)

I:\ATTY\ET\241199US\241199US-AB12.30.07.DOC

VIII. CLAIMS APPENDIX

Claim 1: An encryption apparatus for performing an encryption operation using a public key encryption technique, said encryption apparatus comprising:

public key encryption processing means for performing an encryption operation on data using a public key encryption technique to generate encrypted data;

hash value generation means for generating a hash value which is used by the public key encryption processing means;

storage means for storing the hash value; and

control means for controlling the hash value generation means and the public key encryption processing means, the control means suppressing arithmetic operations performed by the public key encryption processing means when the hash value generation means accesses the storage means.

Claim 2: An encryption apparatus according to claim 1, wherein the public key encryption processing means includes a register group having a register for maintaining an arithmetic operation value and a register for storing a result, the hash value generation means includes a register group having a register for maintaining an arithmetic operation value and a register for storing the generated hash value, at least the register group of the public key encryption processing means and the register group of the hash value generation means are shared, and the hardware is switched in a time-shared manner depending upon the operation mode.

Claim 3: An encryption apparatus according to claim 1, further comprising:

common key encryption processing means for performing an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing means, the common key encryption processing means including a register group having a register for maintaining the resulting data and a register for maintaining key data, wherein the register group of the common key encryption processing means and the register group of the public key encryption processing means are shared.

Claim 4: An encryption apparatus according to claim 3, wherein the common key encryption processing means performs the encryption operation using the DES technique.

Claim 5: An encryption apparatus according to claim 1, wherein the public key encryption processing means includes public key encryption arithmetic operation core means for performing various arithmetic operations for public key encryption, the hash value generation means includes hash value arithmetic operation core means for performing various arithmetic operations for hash value generation, and the public key encryption arithmetic operation core means and the hash value arithmetic operation core means are shared.

Claim 6: An encryption apparatus according to claim 5, wherein the public key encryption arithmetic operation core means includes adder means, and shares the adder means with the hash value arithmetic operation core means.

Claim 7: An encryption apparatus according to claim 1, wherein the public key encryption processing means includes a bus switch for making the bit width variable, and the public key encryption processing means shares the bus switch with the hash value generation means.

Claim 8: An encryption apparatus according to claim 7, further comprising:

common key encryption processing means for performing an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing means, the common key encryption processing means including a bus switch, wherein the bus switch of the common key encryption processing means and the bus switch of the public key encryption processing means are shared.

Claim 9: An encryption apparatus according to claim 1, wherein the hash value generation means stores the generated hash value into the storage means at an address which is used by the public key encryption processing means, and the public key encryption processing means reads the hash value stored in the storage means.

Claim 10: An encryption apparatus according to claim 1, wherein the public key encryption processing means performs the encryption operation using the elliptic curve cryptosystem technique.

Claim 11: An encryption apparatus according to claim 1, wherein the hash value generation means performs an operation using the SHA-1 technique.

Claim 12: An encryption apparatus according to claim 1, wherein the encryption apparatus is incorporated in a non-contact IC card having a communication function.

Claim 13: An encryption apparatus for performing an encryption operation using a public key encryption technique, said encryption apparatus comprising:

a public key encryption processing unit configured to perform an encryption operation on data using a public key encryption technique to generate encrypted data;

a hash value generation unit configured to generate a hash value which is used by the public key encryption processing unit;

a storage unit configured to store the hash value; and

a control unit configured to control the hash value generation unit and the public key encryption processing unit, the control unit configured to suppress arithmetic operations performed by the public key encryption processing unit when the hash value generation unit accesses the storage unit.

Claim 14: An encryption apparatus according to claim 13, wherein the public key encryption processing unit includes a register group having a register configured to maintain an arithmetic operation value and a register configured to store a result, the hash value generation unit includes a register group having a register configured to maintain an arithmetic operation value and a register configured to store the generated hash value, at least the register group of the public key encryption processing unit and the register group of the hash value generation unit are configured to be shared, and the hardware is configured to be switched in a time-shared manner depending upon the operation mode.

Claim 15: An encryption apparatus according to claim 13, further comprising:

a common key encryption processing unit configured to perform an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing unit, the common key encryption processing unit including a register group having a register configured to maintain the resulting data and a register configured to maintain key data, wherein the register group of the common key encryption processing unit and the register group of the public key encryption processing unit are shared.

Claim 16: An encryption apparatus according to claim 15, wherein the common key encryption processing unit is configured to perform the encryption operation using the DES technique.

Claim 17: An encryption apparatus according to claim 13, wherein the public key encryption processing unit includes a public key encryption arithmetic operation core unit configured to perform various arithmetic operations for public key encryption, the hash value generation unit includes a hash value arithmetic operation core unit configured to perform various arithmetic operations for hash value generation, and the public key encryption arithmetic operation core unit and the hash value arithmetic operation core unit are shared.

Claim 18: An encryption apparatus according to claim 17, wherein the public key encryption arithmetic operation core unit includes an adder, and public key encryption arithmetic operation core unit is configured to share the adder with the hash value arithmetic operation core unit.

Claim 19: An encryption apparatus according to claim 13, wherein the public key encryption processing unit includes a bus switch for making the bit width variable, and the public key encryption processing unit is configured to share the bus switch with the hash value generation unit.

Claim 20: An encryption apparatus according to claim 19, further comprising:

a common key encryption processing unit configured to perform an encryption operation using a common key encryption technique to generate a random number for use in the encryption operation of the public key encryption processing unit, the common key encryption processing unit including a bus switch, wherein the bus switch of the common key encryption processing unit and the bus switch of the public key encryption processing unit are shared.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.